УДК 004.04

ТЕНДЕНЦІЇ РОЗВИТКУ ЗАГРОЗ КІБЕРБЕЗПЕЦІ

TRENDS OF CYBERSECURITY THREATES

Павло Кіндрат

Рівненський державний гуманітарний університет,
вул. Степана Бандери 12, м. Рівне, 33028, Україна

Abstract. *The innovative changes that occurred in 2022-23 have significantly shifted the focus of cybersecurity threats, which is evidenced by the statistics on the emergence and realization of information security threats. To successfully counter information threats in the future, it is essential to understand the causes and trends in the development of cyberspace.*

Передумовою до змін у сфері кібербезпеки є не лише самоочевидні чинники розвитку комунікаційних та обчислювальних засобів, а й розвиток суспільства як соціальної категорії, зростання ролі інформаційних технологій у повсякденному житті кожної людини та загальна низька підготовленість людства до викликів, які породжуються такими змінами.

Аналізуючи статистичні звіти щодо динаміки розвитку кіберзагроз за 2022-23 роки можна відмітити кореляцію між суттєвими змінами у спрямованості зловмисної діяльності та як новими технологічними інноваціями, так і модифікацією політичних і соціальних парадигм. Накопичення та аналіз такого роду статистичних даних є критично важливим для покращення розуміння того які аспекти розвитку інформаційних технологій викликатимуть найбільше занепокоєння в майбутньому та завчасно підготуватись до їх викликів.

Основною інновацією яка вплинула на сферу кібербезпеки стало представлення широкій публіці генеративних мовних моделей, які відобразили значний прогрес у розвитку штучного інтелекту. Хоч сама технологія не несе безпосередньої загрози кібербезпеці, вона може широко застосовуватись в удосконаленні та підвищенні ефективності методів соціальної інженерії та атак що використовують ці методи. Похідним наслідком став також стрімкий розвиток та здешевлення апаратних рішень для навчання штучного інтелекту (ШІ) та його підтримки, що зробило технологію більш доступною для широкого вжитку. Зважаючи на особливості організації та функціонування відповідних програмно-апаратних рішень відбувається зростання кількості атак спрямованих не так на заволодіння інформацією, як на знищення її та підтримуючої інформаційної інфраструктури.

Іншою технологічною інновацією, яка проте не мала такого публічного ефекту як ШІ є демонстрація діючих квантових комп'ютерів, що ознаменувало відчутний прогрес у розвитку квантових обчислень. Це, в свою чергу, актуалізувало і прискорило перехід до використання алгоритмів пост-квантової криптографії. Адже попри те, що теоретичні розробки та окремі стандарти в цій галузі існують вже певний час, стандартизація протоколів шифрування і їх застосування в програмному забезпеченні до недавнього часу не отримало широкого вжитку. Збільшення зацікавленості компаній-постачальників інформаційних послуг у впровадженні відповідних алгоритмів у свої продукти спричинило у 2023 році зміщення фокусу кібератак зі спроб отримання фінансової вигоди шляхом використання крипто вимагачів (падіння кількості успішних атак на 60%) чи заволодіння фінансовою інформацією (падіння кількості успішних атак на 40%), на заволодіння корпоративною чи персональною інформацію що зберігається, навіть у зашифрованому вигляді (зростання кількості атак на понад 50%). Кіберзлочинці намагаються заволодіти як найбільшою кількістю доступної інформації до завершення пост квантового переходу, щоб в майбутньому, при наявності більш доступних квантових комп'ютерів, мати можливість розшифрувати накопичені дані і отримати від них вигоду.